

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日            2 0 0 3 年 1 0 月 2 8 日  
Date of Application:

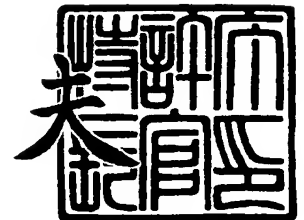
出 願 番 号            特 願 2 0 0 3 - 3 6 7 1 5 2  
Application Number:  
[ST. 10/C]:            [ J P 2 0 0 3 - 3 6 7 1 5 2 ]

出 願 人            株式会社日立製作所  
Applicant(s):

2 0 0 3 年 1 2 月    4 日

特許庁長官  
Commissioner,  
Japan Patent Office

今 井 康



【書類名】 特許願  
【整理番号】 NT03P0753  
【提出日】 平成15年10月28日  
【あて先】 特許庁長官 殿  
【国際特許分類】 G06F 3/06  
【発明者】  
    【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日立製作所  
                        システム開発研究所内  
    【氏名】 白銀 哲也  
【特許出願人】  
    【識別番号】 000005108  
    【氏名又は名称】 株式会社日立製作所  
【代理人】  
    【識別番号】 100068504  
    【弁理士】  
    【氏名又は名称】 小川 勝男  
    【電話番号】 03-3661-0071  
【選任した代理人】  
    【識別番号】 100086656  
    【弁理士】  
    【氏名又は名称】 田中 恭助  
    【電話番号】 03-3661-0071  
【選任した代理人】  
    【識別番号】 100094352  
    【弁理士】  
    【氏名又は名称】 佐々木 孝  
    【電話番号】 03-3661-0071  
【手数料の表示】  
    【予納台帳番号】 081423  
    【納付金額】 21,000円  
【提出物件の目録】  
    【物件名】 特許請求の範囲 1  
    【物件名】 明細書 1  
    【物件名】 図面 1  
    【物件名】 要約書 1

**【書類名】 特許請求の範囲****【請求項 1】**

IP ネットワークを介して接続されるホストコンピュータから送信されるコマンドを処理するストレージ装置において、  
該コマンドによって処理される対象となるデータを記憶する記憶装置と、  
該ホストコンピュータの識別に関連する第一の情報を格納するアクセス管理テーブルを保持するメモリと、  
該ホストコンピュータから送信されるログイン要求に関して、該ログイン要求のフレームに該ホストコンピュータの識別に関連する第二の情報が含まれるか否かを判定する第一判定手段と、  
該第一判定手段による判定の結果、該ログイン要求フレームに、意図する第二の情報が含まれていない場合には、該ログイン要求フレームのソースアドレスに対してホストコンピュータの識別に関連する第一の情報を送信するように要求する手段と、  
該要求手段からの要求に対する応答として、該ホストコンピュータから獲得した第一の情報に関して、該アクセス管理テーブルを参照して判定する第二判定手段と、  
該第二判定手段による判定の結果に応じて、該ログイン要求の許可を行うことを特徴とするストレージ装置。

**【請求項 2】**

該記憶装置は、iSCSI プロトコルによりアクセスさせることを特徴とする請求項 1 記載のストレージ装置。

**【請求項 3】**

前記アクセス管理テーブルに格納される第一の情報は、ホストコンピュータが接続される IP ネットワークのインタフェースの MAC アドレスである請求項 1 又は 2 記載のストレージ装置。

**【請求項 4】**

該ストレージ装置は、IP ネットワークに接続される装置を監視するための SNMP マネージャを有し、該 SNMP マネージャは、該ホストコンピュータから第一の情報を送信するように要求するフレームを、該ホストコンピュータに関係するインタフェースの MIB を要求する SNMP リクエストとして送信することを特徴とする請求項 1 乃至 3 のいずれか記載のストレージ装置。

**【請求項 5】**

該ストレージ装置は更に、前記アクセス管理テーブルの内容を変更するための入出力を行うコンソールを備えることを特徴とする請求項 1 乃至 3 のいずれかに記載のストレージ装置。

**【請求項 6】**

前記第二の判定手段による判定で、前記アクセス管理テーブルにホストコンピュータを識別する第一の情報が格納されていないと判定した場合に、該ログイン要求の内容をログとして前記メモリに格納する請求項 1 乃至 3 のいずれかに記載のストレージ装置。

**【請求項 7】**

前記第二の判定手段による判定で、該アクセス管理テーブルに該ホストコンピュータを識別する第一の情報が格納されていると判定した場合、該ログイン要求フレームのソース IP アドレスを、ホストコンピュータを識別する前記情報と関連付けて該アクセス管理テーブルに格納する請求項 3 記載のストレージ装置。

**【請求項 8】**

該アクセス管理テーブルには、MAC アドレスと、該 MAC アドレスの IP ネットワークのインタフェースを持つホストコンピュータがアクセス許可された論理装置 (LU) の識別符号が登録されており、  
該ホストコンピュータから送信されたコマンドの処理に関して、予め許可された論理装置へのアクセスか否かの判定を行ない、許可された論理装置に対して該コマンドの処理を行なうことを特徴とする請求項 3 記載のストレージ装置。

**【請求項 9】**

該アクセス管理テーブルには、該MACアドレスに関連付けた該MACアドレスのIPネットワークインタフェースを持つホストコンピュータのIPアドレスが格納される請求項3又は8記載ストレージ装置。

**【請求項 10】**

外部の装置からネットワークを介してストレージ装置へ送られるアクセス要求に関して、アクセス許可を管理するアクセス制御の管理方法において、  
外部から送信されるログイン要求のフレームをストレージ装置で受信するステップと、  
受信した該フレームに該外部の装置を特定する第二の情報が含まれているかを判定する第一の判定ステップと、  
第一の判定の結果、該フレームに該第二の情報が含まれていない場合、該外部の装置に対してそれを特定する第一の情報の取得を要求するステップと、  
取得された該第一の情報に関してチェックを行い、アクセス許可をすべきかを判定する第二の判定ステップと、  
該第二の判定の結果、許可された場合に該外部の装置からストレージ装置に対するアクセス要求を許可するステップと、  
を有することを特徴とするアクセス制御管理方法。

**【請求項 11】**

前記第一の情報としてMACアドレスを使用し、前記第二の情報としてIPアドレスを使用する請求項10記載のアクセス制御管理方法。

**【請求項 12】**

該ストレージ装置へのアクセスが許可された外部装置を特定する第一の情報を登録するテーブルをメモリに予め用意するステップを有し、  
前記第二の判定ステップは、外部装置から取得された第一の情報に関して、該テーブルを参照することにより判定を行うことを特徴とする請求項9記載のアクセス制御管理方法。

**【請求項 13】**

前記第一の判定ステップによる判定の結果、又は第二の判定ステップによる判定の結果、不適合の場合、受信されたログイン要求のフレームに関する情報をログとしてメモリに格納するステップを有することを特徴とする請求項9記載のアクセス制御管理方法。

**【請求項 14】**

前記第一の情報の取得を要求ステップにおいて、IPネットワークに接続される装置を監視するためのSNMPマネージャにより該外部の装置から第一の情報を送信するように要求することを特徴とする請求項9記載のアクセス制御管理方法。

**【請求項 15】**

前記第一の情報の取得を要求ステップにおいて、iSCSIのTEXT Mode negotiationによるプロトコルを用いて該外部の装置からMACアドレスを得ることを要求することを特徴とする請求項9記載のアクセス制御管理方法。

**【請求項 16】**

該ストレージ装置に複数の論理装置(LU)を定義するステップと、  
MACアドレスと、MACアドレスのIPネットワークのインタフェースを持つ外部の装置がアクセス許可されたLUの識別符号が登録されたアクセス管理テーブルを用意するステップと、  
前記第二の判定ステップの後に、外部の装置から送信されたコマンドの処理に関して、該テーブルを参照して予め登録されたLUに対するアクセスか否かを判定する第三の判定ステップと、を有し、  
該第三の判定の結果、許可されたLUに対して該コマンドの処理を行なうことを特徴とする請求項12記載のアクセス制御管理方法。

**【請求項 17】**

ネットワークに接続された第一の装置から第二の装置へのアクセスに関する許可を管理する方法において、

第一の装置から第二の装置に対するアクセスが同一のネットワーク間で行われるか否かを該第一の装置から送信される第二の情報を用いてチェックする第一のチェックモードと、該第一のチェックモードにおいて、同一のネットワーク間の通信でないと判定された場合、送信元となる該第一の装置から所定の第一の情報を獲得するステップと、獲得された該第一の情報を用いて該第二の装置へのアクセスの許可の可否をチェックする第二のチェックモードと、該第二のチェックモードにおいて許可された場合に、該第一の装置から該第二の装置へ送信されるコマンドの処理を行うことを特徴とするアクセスの管理方法。

【請求項 1 8】

前記第一の装置はホストコンピュータであり、第二の装置は複数の論理装置が規定され、iSCSI プロトコルによりコマンド処理されるストレージ装置であり、該第一の情報は MAC アドレスであり、該第二の情報は該第一の装置から送信されたフレームに含まれる IP アドレスである請求項 1 7 記載のアクセスの管理方法。

【請求項 1 9】

iSCSI 層、TCP 層、IP 層、データリンク層を有するストレージ装置を IP ネットワークに接続するステップを更に有すること特徴とする請求項 1 0 又は 1 8 記載のアクセスの管理方法。

【請求項 2 0】

iSCSI イニシエータを有する第一の装置と、iSCSI ターゲットを有する第二の装置との間で IP ネットワークを介して通信を行って、コマンドの処理を行う方法において、第一の装置から送信されるログイン要求のフレームを第二の装置で受信し、受信した該フレームに該第一の装置を特定する所定の情報が含まれているかをチェックし、該チェックの結果、該フレームに該所定の情報が含まれていない場合、該第二の装置から該第一の装置に対して該第一の装置を特定する他の所定の情報の取得を要求し、該第一の装置から第二の装置へ送信された他の所定の情報に関して、該第一の装置からのアクセスを許可すべきか否かをチェックし、該チェックの結果、許可された場合に該第一の装置から送信されるコマンドを該第二の装置の iSCSI 上で処理することを特徴とするコマンドの処理方法。

【請求項 2 1】

該第一の装置に備えられる SNMP エージェントと、該第二の装置に備えられる SNMP マネージャとの間の通信により他の所定の情報である MAC アドレスの取得が行われることを特徴とする請求項 2 0 記載のコマンドの処理方法。

【請求項 2 2】

IP ネットワークを介して接続されるホストコンピュータから送信されるコマンドを処理するストレージ装置において、該コマンドによって処理される対象となるデータを記憶する記憶装置と、該ホストコンピュータの識別に関連する第一の情報を格納するアクセス管理テーブルを保持するメモリと、該ホストコンピュータからの要求を処理する処理装置とを有し、該処理装置は、該ホストコンピュータから送信されるログイン要求に関して、該ログイン要求のフレームに該ホストコンピュータの識別に関連する第二の情報が含まれるか否かを判定し（第一の判定）、該第一の判定の結果、該ログイン要求フレームに、意図する第二の情報が含まれていない場合には、該ログイン要求フレームのソースアドレスに対してホストコンピュータの識別に関連する第一の情報を送信するように要求し、該要求手段からの要求に対する応答として、該ホストコンピュータから獲得した第一の情報に関して該アクセス管理テーブルを参照して判定し（第二の判定）、該第二の判定の結果に応じて、該ログイン要求の許可を行うことを特徴とするストレージ装置。

**【書類名】 明細書****【発明の名称】 ストレージ装置及びそのアクセス管理方法****【技術分野】****【0 0 0 1】**

本発明は、ストレージ装置及びそのアクセス管理方法に係り、特にホストコンピュータ（以下単にホストと言う）からiSCSIプロトコルによってストレージ装置内のデータをアクセスするストレージシステムにおけるセキュリティの管理に関する。

**【背景技術】****【0 0 0 2】**

単体又は複数のハードディスクドライブの集合体、若しくは専用の制御部で複数のハードディスクドライブを制御するディスクアレイ装置等から成るストレージ装置（記憶装置システム）を、インタフェースを介してホストと接続して、ホストからアクセスするストレージシステムが実用化されている。通常、ストレージ装置は、1つ又は複数のボリュームと称する論理装置（Logical Unit: L U）を持ち、論理装置には I D 番号又は論理装置番号（L U N）が割当てられる。

**【0 0 0 3】**

ストレージ装置とホストを接続するインタフェース技術としては、SCSI（Small Computer Systems Interface）やファイバチャネル（FC）が用いられる。SCSIインタフェースは安価であり、クライアント/サーバ型を基本とする比較的近距離接続用のインタフェースとして利用されている。SCSIにおいて、クライアントはコマンドを発行する能動的な役割を持ち、イニシエタと呼ばれる。またサーバは、クライアントの要求に従う受動的な役割を持ち、ターゲットと呼ばれる。論理装置に処理を指示するコマンドは、イニシエタから発行されるCommand Descriptor Block（CDB）に含まれる。

**【0 0 0 4】**

このようなストレージシステムにおいて、ストレージ装置内の論理装置（L U）に対する不正なアクセスを防止するためのセキュリティを実現する技術としては、例えば、特開平 1 0 - 3 3 3 8 3 9 公報（特許文献 1）或いは特開 2 0 0 1 - 2 6 5 6 5 5 公報（特許文献 2）に開示されている。

**【0 0 0 5】**

前者は、L U 毎に予めアクセス許可したホストを示すWWN（World Wide Name）との関係をストレージ装置内のテーブルに記憶しておき、ホストからのログインフレームに格納されたWWNとテーブルの内容とを照合することによってホストの識別を行い、ストレージ装置内のL Uへのアクセス可否の判断を行なう。

**【0 0 0 6】**

後者は、ホストのWWNとポート I D の関係をテーブルに記憶し、WWNが格納されていないフレーム（たとえばCDBが格納されたフレーム）について、ポート I D から対応するWWNを参照してL Uのアクセス可否の判断を行なう。  
なお以下、ストレージ装置内の特定L Uに対するホストからのアクセス可否を制御する方法を、便宜上「L U Nセキュリティ」と呼ぶことにする。

**【0 0 0 7】**

ところで、最近、ネットワークプロトコルであるTCP/IP上で、上位プロトコルとしてSCSI処理を実現するためのプロトコル技術であるiSCSI（internet S C S I）が注目されている。iSCSIはIPネットワーク上で用いられるプロトコルとして、IETF（The Internet Engineering Task Force）で規格化されたものである。

**【0 0 0 8】**

【特許文献 1】 特開平 1 0 - 3 3 3 8 3 9 公報

**【0 0 0 9】**

【特許文献 2】 特開 2 0 0 1 - 2 6 5 6 5 5 公報

**【発明の開示】****【発明が解決しようとする課題】**

**【0010】**

IPネットワークはファイバチャネルよりも安価であり、より多くのユーザからストレージ装置内のLUを利用する形態が取り得ると考えられる。しかし、誤操作や悪意のある攻撃によってLUのデータが破壊されてしまった場合に影響を及ぼす範囲も広がる。このため、IPネットワーク上でiSCSIを用いたストレージ装置内のLUに対するアクセスにおいてもLUNセキュリティを保証することが重要である。

**【0011】**

LUNセキュリティのチェックのために、TCP/IPで知られているMACアドレスをホスト識別情報として用いることが考えられる。MACアドレスは、ビット数が比較的少なく、アクセス管理のために必要な記憶領域が少なく済み、また物理的なネットワークインタフェースに固有の値であるので、詐称されにくい、という利点を持つ。

**【0012】**

しかしながら、IPネットワークにおいて、ルータを経由するとデータリンクフレームのMACアドレスはルータのネットワークカードのMACアドレスに書き換えられてしまう。従って、ホストとストレージ装置の間にルータがある場合、ターゲットはホストから受信したパケットからホストのMACアドレスを取得できないという問題がある。

**【0013】**

上記特許文献1及び文献2には、IPネットワークでMACアドレスをホスト識別のための情報として利用するに際して、ルータを経由する場合のMACアドレスを取得する方法についてまでは言及されていない。

**【0014】**

本発明の目的は、iSCSIプロトコルを用いるストレージ装置に対するホストからのアクセス要求に関するセキュリティの向上を図ったアクセスの管理方法又はストレージ装置を提供することにある。

本発明の他の目的は、IPネットワークに接続されたストレージ装置において、MACアドレスを用いてホストを識別して、ホストからのログイン要求の許可の判定を行い得る方法又はストレージ装置を提供することにある。

本発明の他の目的は、IPネットワークに接続されるストレージ装置に対するアクセスに関し、アクセス元のホストが同一のネットワークに属するか否かに応じて、ログイン要求処理やコマンドに関するアクセス管理の方法を変更することができるアクセスの管理方法を提供することにある。

**【課題を解決するための手段】****【0015】**

本発明は、IPネットワークを介して接続されるホストコンピュータから送信されるコマンドを処理するストレージ装置において、コマンドによって処理される対象となるデータを記憶する記憶装置と、ホストコンピュータの識別に関連する第一の情報を格納するアクセス管理テーブルを保持するメモリと、ホストコンピュータから送信されるログイン要求に関して、ログイン要求のフレームにホストコンピュータの識別に関連する第二の情報が含まれるか否かを判定する第一判定手段と、第一判定手段による判定の結果、ログイン要求フレームに意図する第二の情報が含まれていない場合には、ログイン要求フレームのソースアドレスに対してホストコンピュータの識別に関連する第一の情報を送信するように要求する手段と、要求手段からの要求に対する応答として、ホストコンピュータから獲得した第一の情報に関して、アクセス管理テーブルを参照して判定する第二判定手段と、第二判定手段による判定の結果に応じて、ログイン要求の許可を行うものである。

好ましい例では、上記記憶装置は、iSCSIプロトコルによりアクセスさせる。また、上記アクセス管理テーブルに格納される第一の情報は、ホストコンピュータが接続されるIPネットワークのインタフェースのMACアドレスである。

**【0016】**

本発明に係るアクセス管理方法は、外部の装置例えばホストコンピュータからネットワークを介してストレージ装置へ送られるアクセス要求に関して、アクセス許可を管理する

アクセス制御の管理方法において、外部から送信されるログイン要求のフレームをストレージ装置で受信するステップと、受信した該フレームに外部の装置を特定する第二の情報が含まれているかを判定する第一の判定ステップと、第一の判定の結果、フレームに第二の情報が含まれていない場合、外部の装置に対してそれを特定する第一の情報の取得を要求するステップと、取得された第一の情報に関してチェックを行い、アクセス許可をすべきかを判定する第二の判定ステップと、第二の判定の結果、許可された場合に外部の装置からストレージ装置に対するアクセス要求を許可するステップとを有する。

#### 【0017】

好ましい例において、ストレージ装置は、iSCSI層、TCP層、IP層、データリンク層を有し、このストレージ装置をIPネットワークに接続される。

第一の情報として、好ましくはMACアドレスが使用され、第二の情報としてIPアドレスが使用される。

また、好ましくは、ストレージ装置へのアクセスが許可された外部装置を特定するMACアドレスを登録するテーブルが、ストレージ装置のメモリに予め用意される。そして、第二の判定ステップでは、外部装置から取得された第一の情報に関して、このテーブルを参照することにより判定が行なわれる。

また、第一の情報の取得を要求ステップにおいて、IPネットワークに接続される装置を監視するためのSNMPマネージャにより外部の装置から第一の情報を送信するように要求する。

#### 【0018】

好ましい例では、ストレージ装置には、複数の論理装置(LU)が定義され、またアクセス管理テーブルには、MACアドレスと、MACアドレスのIPネットワークのインタフェースを持つ外部の装置がアクセス許可されたLUの識別符号が登録される。そして、前記第二の判定ステップの後に、外部の装置から送信されたコマンドの処理に関して、このテーブルを参照して予め登録されたLUに対するアクセス可否かを判定する第三の判定ステップを有し、この第三の判定の結果、許可されたLUに対してコマンドの処理が行なわれる。

#### 【0019】

本発明はまた、ネットワークに接続された第一の装置から第二の装置へのアクセスに関する許可を管理する方法、或いはコマンド処理の方法として把握される。この方法は、第一の装置から第二の装置に対するアクセスが同一のネットワーク間で行われるか否かを第一の装置から送信された情報のうちの第二の情報を用いてチェックする第一のチェックモードと、第一のチェックモードにおいて、同一のネットワーク間の通信でないと判定された場合、送信元となる第一の装置にから所定の第一の情報を獲得するステップと、獲得された第一の情報を用いて第二の装置へのアクセスの許可の可否をチェックする第二のチェックモードと、第二のチェックモードにおいて許可された場合に、第一の装置から第二の装置へ送信されるコマンドの処理を行う。

#### 【発明の効果】

#### 【0020】

本発明によれば、IPネットワークに接続されたiSCSIプロトコルを用いるストレージ装置において、MACアドレスを用いてホストを識別して、ホストからのログイン要求の許可の判定が行える。

また、アクセス元のホストが同一のネットワーク(同一セグメント)に属するか否かに応じて、ログイン要求処理やコマンドに関するアクセス管理の方法を変更することができる。これにより、ストレージ装置に対するホストからのアクセス要求に関するセキュリティの向上が図れる。

#### 【発明を実施するための最良の形態】

#### 【0021】

以下、図面を参照して本発明の実施形態を説明する。

図1は一実施形態によるデータ処理システムのハードウェア構成を示すブロック図である



。このデータ処理システムは、IPネットワーク400を介してホスト100とストレージ装置200が接続されて構成される。このネットワーク400を介してホスト100とストレージ装置200の間でパケット形式のデータが送受信される。

#### 【0022】

ストレージ装置200は、記憶制御装置210、複数のディスク装置220及びサービスプロセッサ(SVP)230を備える。複数のディスク装置は、大量のデータを記憶する例えばRAID構成のディスクアレイ装置であり、ホストからのコマンド処理によりデータの書き込み読み出しが行われる。SVP230は表示部及び入力部を備える。記憶制御装置210は、ホストアダプタ240、キャッシュメモリ250、ディスクアダプタ260、プロセッサ270、制御メモリ280を有する。ホストアダプタ240は、iSCSIポート242を有する。ポート211はギガビットイーサネットのような高速IPインタフェース410を介してIPネットワーク400に接続される。

#### 【0023】

ホスト100は、CPU110、主記憶装置120、及び入出力処理装置130を有する計算機であり、具体的にはワークステーション、マイクロコンピュータ又はメインフレームコンピュータ等である。入出力処理装置130は、iSCSIポート132を有する。ポート132は高速IPインタフェース410を介してIPネットワーク400に接続される。

#### 【0024】

尚、図示していないが、ホスト100とストレージ装置200は、ルータを介してIPネットワーク経由400で接続される場合もある。また、接続する経路は一本であるとは限らない。

#### 【0025】

図2は、図1に示すデータ処理システムの論理的な構成を示す図である。ホスト100で生成されたコマンドまたはデータ50は、iSCSI層90AのiSCSIイニシエータ機能でプロトコル変換され、更にTCP層92、IP層94で制御情報(ヘッダ)を付加されてパケット処理され、データリンク層96からネットワーク400へ送信される。データリンク層はMAC(Media Access Control)層とも呼ばれ、例えばイーサネット(登録商標)やギガビットイーサネットとして実現される。

#### 【0026】

一方、ストレージ装置200では、ネットワーク400から受信されたコマンドまたはデータ50は、データリンク層96、IP層94、TCP層92で処理され、各制御情報を除去される。そして、イニシエータのiSCSIイニシエータ機能が送り出した形でiSCSI層90BのiSCSIターゲット機能へと送られ、処理される。各プロトコル処理層すなわちiSCSI層、TCP層、IP層、データリンク層はハードウェアまたはプロセッサ上のソフトウェア、あるいはそれらの組み合わせにより実現される。

尚、ストレージ装置200からホスト100へデータが送信される時は、上記と逆のプロトコル処理が行われる。

#### 【0027】

本実施例で特徴的なことは、ホスト100には、SNMPエージェント99Aが実装され、ストレージ装置200にSNMPマネージャ99Bが実装される。そのために、ホスト100とストレージ装置200は、夫々UDP層98を持つ。また、ストレージ装置200は、ホストを一意に識別する情報を格納するアクセス管理テーブル80を有する。尚、アクセス管理テーブル80の内容については図5を参照して後述する。

#### 【0028】

ここで、SNMP(Simple Network Management Protocol)の一般的な効用について概略説明しておきたい。

SNMPは、IETF規格でRFC1157として定義された、ネットワークに接続された機器をネットワーク経由で監視するためのプロトコルであり、UDP/IP上で規定されて使用される。SNMPは管理対象となる機器に常駐するSNMPエージェントと、管理する側の機器(

監視サーバ) 上の SNMP マネージャ間で通信に用いられる。SNMP マネージャと SNMP エージェントの間で行われる通信には 3 つの種類があるが、その内この実施例では、情報の要求と応答に関する通信の例を用いる。即ち、SNMP マネージャから SNMP エージェントに、監視対象の機器の情報を要求し、一方、SNMP エージェントは要求された情報を取得して SNMP マネージャに応答する。

#### 【0029】

SNMP で管理される機器は、MIB (Management Information Base) と呼ばれる機器の状態を表わすデータと、SNMP マネージャの指示によりこれを実行する SNMP エージェントと呼ばれるプログラムを持つ。MIB として定義されていればポート数など静的で変化の無い情報も、トラフィック状態など動的な情報もいずれも取得可能である。一般に IP ネットワーク管理はネットワーク構成機器が多種・多数で困難な作業となりがちであるが、SNMP と MIB を利用することにより効率的な管理ができる。

#### 【0030】

SNMP 処理や UDP プロトコル処理に関しては、各プロトコル処理層すなわち iSCSI 層、TCP 層、IP 層、データリンク層の処理と同様にハードウェアまたはプロセッサ上のソフトウェア、あるいはそれらの組み合わせで実現される。例えば SNMP マネージャ 99B および SNMP エージェント 99A としては、既に用意されているソフトウェアを用いても良い。例えばホスト 100 の OS が Linux ならば、Linux 用に公開されているプログラムを入手してインストールして、適当に MIB を設定する。

#### 【0031】

本実施例では、SNMP マネージャ 99B は MAC アドレスを獲得するために使用される。MIB 構造のなかでも MIB-2 で定義される MAC アドレスの獲得にのみ特化した SNMP 機能を部分的にサポートしたソフトウェアとして実現する。この場合、SNMP 機能は iSCSI ターゲットおよび iSCSI イニシエタの機能の一部として実現できる。アクセス要求を送信したホストを識別するために、ホストのポートの MAC アドレスを用いる利点としては、MAC アドレスはビット数が少なくアクセス管理テーブルのために必要な記憶領域が少なく済む。また MAC アドレスはポートに固有の値であるので、詐称されにくいこと、が上げられる。

#### 【0032】

次に、ホスト 100 の SNMP エージェントとストレージ装置 200 SNMP マネージャとの間の通信について簡単に説明する。(詳細は図 6～8 を参照して後述する。) ホスト 100 から送信された iSCSI ログイン要求 S1 を受信したストレージ装置の iSCSI ターゲット機能 90B は、SNMP マネージャ 99B に指示して、iSCSI ログイン要求 S1 の発行元のネットワークアドレス (IP アドレス) に対し MAC アドレスを要求するために、SNMP リクエスト S2 を送信させる。

SNMP リクエスト S2 を受信したホスト 100 の SNMP エージェント 99A は、通常の SNMP 処理として、要求された MAC アドレスを含む MIB を SNMP レスポンス S3 として応答する。この SNMP レスポンス S3 を受信した SNMP マネージャ 99B は、iSCSI ターゲット機能 90B へ受信した MAC アドレスを報告する。

#### 【0033】

iSCSI ターゲット機能 90B は、獲得したホストの MAC アドレスが、アクセス管理テーブル 80 に登録されているか否かによりログインが正当であるか否かの判定を行なう。アクセス管理テーブル 80 にその MAC アドレスが登録されている場合には、ログイン要求を許可し、それを伝えるためホストにログインレスポンスを返信する (S4)。また、この様にしてログインが成立した後、ホストから受信するコマンドについて、予め許可された LU へのアクセスか否かの判定を行ない、許可された LU に対するコマンドの処理を行なう。尚、このアクセス制御処理の詳細については後述する。

#### 【0034】

図 3 は、iSCSI のイニシエタとターゲット間の通信に用いられるパケットのフォーマットの例を示す。

iSCSI層において、データの通信の単位となる P D U (iSCSI PDU) は、BHS (Basic Header Segment) 3 3 とデータセグメント 3 4 から構成される。BHS 3 3 とデータセグメント 3 4 との間に AHS (Additional Header Sequence) が挿入される場合もあるが、図 3 の例ではそれを省略してある。

#### 【 0 0 3 5 】

TCP層、IP層、データリンク層では、iSCSI層からのパケットデータに対して先頭に、データリンクヘッダ (DLH) 3 0、IPヘッダ (IPH) 3 1、TCPヘッダ (TCH) 3 2 が付加される。さらに iSCSIパケットデータの最後部にはデータリンクトレイラ (DLT) 3 5 が付加される。

#### 【 0 0 3 6 】

IP層では、IPアドレスと呼ぶ番号でノード (ネットワークに接続されている機器) の識別が行なわれる。現在広く普及している IPv4 では、IPアドレスとして 32 ビットの数値が使われており、次世代の IPv6 では 128 ビットの数値が用いられる。IPv4 の IPヘッダでは先頭から 13 ~ 16 バイト目に発信元を示すソース IP アドレスが格納され、17 ~ 20 バイト目に宛先を示すデスティネーション IP アドレスが格納される。

#### 【 0 0 3 7 】

データリンク層において、各ネットワークカードには固有のアドレスが割り当てられ、このアドレスを基にしてデータリンクフレーム (データリンクヘッダから始まりデータリンクトレイラで終了する) の送受信が行なわれる。この固有のアドレスを MAC アドレスと呼ぶ。MAC アドレスはイーサネットならば 6 バイト長であり、先頭の 3 バイトはベンダコードとして IEEE (Institute of Electrical and Electronic Engineers) が管理し割り当てを行なっている。残り 3 バイトは各ベンダで重複しないように管理しているコードである。このようにして設定された MAC アドレスは、他人の MAC アドレスとは重複せず、全て異なるアドレスが割り当てられる。

#### 【 0 0 3 8 】

データリンクヘッダの最初の 6 バイトは宛先を示すデスティネーション MAC アドレスである。データリンクヘッダの次の 6 バイトは発信元を示すソース MAC アドレスである。

#### 【 0 0 3 9 】

図 4 に、ログイン要求フレームの構成例を示す。

ログイン要求或いはログインレスポンスのフレームは、基本的に似ている。図 4 は、ログイン要求、ログインレスポンスフレームの、主に iSCSI の P D U の部分を示す。いずれのフレームも 1 ワードが 4 バイトずつで、BHS は 4 8 ワードから構成されている。

#### 【 0 0 4 0 】

BHS の後にはデータセグメントが付加される。ログイン要求フレームおよびログインレスポンスフレームでは、データセグメントに iSCSI 通信に必要な各種パラメータを格納して、それらの交換やネゴシエーションを行う。パラメータは、TEXT 形式と呼ぶ、< キー > = < 値 > で表される形式で記述される。データセグメントは可変長 (4 バイトの倍数) である。

#### 【 0 0 4 1 】

ログインレスポンスのステータス領域 (Status-Class と Status-Detail を合せた領域) にはログインのステータスが格納される。ステータスが 0 0 0 0 (Status-Class 及び Status-Detail が 0 0) ならば、ログインが成功している状態を示す。ステータスが 0 0 0 0 以外ならば何らかの理由でログインが成功していない状態を示し、イニシエタは別のパラメータでログインを試みるか、或いはログインをあきらめる。

#### 【 0 0 4 2 】

次に、図 5 を参照してアクセス管理テーブル 8 0 について説明する。アクセス管理テーブル 8 0 には、各行ごとにホストのネットワークインタフェースの MAC アドレス 81 と、それに対応する IP アドレス 82 と、MAC アドレスを持つホストに対しアクセス許可する LU のリスト 83 と、MAC アドレスを持つホストとの通信状況 (Session

)84が登録される。

#### 【0043】

通信状況84は、例えば次の様に表される。

(1) iSCSIログイン要求受信前であってホストとの通信が行なわれていない ("not establish")

(2) iSCSIログイン要求を受信して判定中であり、iSCSIログインレスポンスを応答してログイン成立前 ("login")

(3) iSCSIログイン成立後 ("establish")

アクセス管理テーブル80は、ホストとアクセスを許されたLUをアクセス管理テーブルに設定するために、それらの内容をコンソールSV P 2 3 0の表示部に表示したり、その入力部からの操作により登録内容の変更が可能である。

#### 【0044】

次に図6～図8のフローチャートを参照して、アクセス制御処理の詳細について説明する。

ストレージ装置100は、ホスト100から送信されたiSCSI Login 要求S1を受信すると(1100)、そのiSCSI Login 要求S1のIPヘッダを参照して、ソースアドレスが自ポートと同一セグメント内のIPアドレスであるか否かを判定する(1110)。

この判定の結果、iSCSI Login 要求S1のソースIPアドレスが自ポートと同一ネットワーク内で無かった場合、同一ネットワーク外のポートからログイン要求があったことを制御メモリ280内のログに記録する(1120)。そしてSNMPマネージャ99Bに、iSCSI Login 要求フレームのソースIPアドレスに対するMIB獲得を指示する(1130)。この指示に従って、SNMPマネージャ99Bは、SNMPリクエストS2をホストへ送信する。

#### 【0045】

次に、ホスト100でSNMPリクエストが拒絶されたか又はSNMPレスポンスがホストから応答されず一定時間経過した(タイムアウトが発生した)か否かが判定される(1140)。もしSNMPリクエストS2に対するSNMPレスポンスS3が、タイムアウトを起こさずにストレージ装置200で受信できた場合、そのSNMPレスポンスで獲得したホストのポートのMACアドレスが、アクセス管理テーブル80に登録されているか否かが判定される(1150)。その判定の結果、テーブル80に登録されている場合には、ホスト100からのアクセスが許可されているため、ログインを許可するiSCSI Login レスポンスS4をホストに対して返信する(1160)。

#### 【0046】

この後は、図6に示すiSCSI の Full Feature phase に移る(1400)。この場合、ログイン要求をしてきたホスト100はストレージ装置200とは異なるセグメントにあるので、ホスト100から送信された各フレームのMACアドレスは途中のルータ装置で書き換えられるため、ホスト識別情報としては、ホスト送信フレームのソースIPアドレスを用いる。

#### 【0047】

ホスト100からCommand PDUを受信したら(1410)、アクセス管理テーブル80を参照して、コマンドが格納されたフレームのソースIPアドレスについて、そのコマンドが示すLUが登録されているか否かを判定する(1420)。この判定の結果、もしLUが登録されていれば、そのLUへのアクセス許可があると判断して、そのLUに対してコマンドの処理を行ない(1430)、そのコマンドの処理を終了する(1440)。

#### 【0048】

一方、ステップ1420の判定において、ソースIPアドレスから、もしコマンドが示すLUが登録されていなければ、そのLUへのアクセスが許可されていないアクセス要求があったことをログに記録し(1450)、そのコマンドの処理を行わずに終了する。

#### 【0049】

さて話を戻して、上記ステップ1110の判定の結果、「Yes」であるときには、図

7に示す処理が行なわれる。この場合、ログイン要求をしてきたホスト100はストレージ装置200と同一セグメントにあるので、ホストから送信された各フレームのソースMACアドレスをホスト識別情報として利用できる。

#### 【0050】

まず、iSCSI Login リクエストS1のソースMACアドレスがアクセス管理テーブル80に登録されているか否かを判定する(1230)。この判定の結果、もしテーブル80に登録されていれば、ホスト100からのアクセスが許可されているので、ログインを許可する旨のiSCSI Login レスポンスS4をホストへ返信する(1240)。この後、iSCSIのFull Feature phaseとなる(1300)。すなわちホスト100からCommand PDUを受信したら(1310)、アクセス管理テーブル80を参照して、そのコマンドが格納されたフレームのソースMACアドレスに関し、コマンドが示すLUが登録されているか否かを判定する(1320)。もしLUが登録されていれば、そのLUに関してコマンドの処理を行ない(1330)、そのコマンドの処理を終了する(1340)。

#### 【0051】

一方、上記ステップ1320の判定で、ソースMACアドレスから、そのコマンドが示すLUが登録されていない場合は、そのLUへのアクセスが許可されていないアクセス要求があったことをログに記録し(1350)、そのコマンドの処理を行わずに終了する。

#### 【0052】

また、上記ステップ1230の判定の結果「No」であった場合、またはステップ1140の判定の結果「Yes」であった場合、またはステップ1150の判定の結果「No」であった場合には、ログインを許可しない旨のiSCSI Login レスポンスをホスト100へ応答(ステータスとして0000以外を応答)する(1200)。すなわちこの場合には、MACアドレスを用いてホストを識別できなかった、或いはホストのMACアドレスがアクセス管理テーブル80に登録されていなかったため、アクセスを許可されていないポートからのログイン要求があったものと判断する。そして未登録のポートからログイン要求があったことをログに記録して終了する(1210)。

#### 【0053】

尚、上記ログに関して言えば、ログとして相手ポートのIPアドレス及びイベントの発生時刻がイベント毎に取得されて、制御メモリ280に記憶される。この様に取得されたログは、その後管理者の操作又は予め定められたスケジュールに従ってSVP230の表示部に表示される。管理者はその表示内容から判断して、ネットワークの切り離しや、及び目的外のホストからのアクセスの防止のための操作を行える。

#### 【0054】

以上、一実施形態について説明したが、以下種々の変形例について説明する。  
上記実施形態では、ステップ1110でiSCSI Login リクエストS1を送信したポートが自ポートと同一セグメントに属するか否かを iSCSI Login リクエストが格納されたIPパケットのソースIPアドレスで判定している。しかしながら変形例では、そのソースIPアドレスに代わって、IPパケットがカプセル化されたイーサネットフレームのフレームヘッダに含まれるソースMACアドレスで判定しても良い。すなわち、ソースMACアドレスが、ルータのポートのMACアドレスである場合、イーサネットフレームはルータを経由して自ポートに到達したので、iSCSI Login リクエストを発行したポートは同一ネットワークに属さない。ソースMACアドレスが、ルータのポートのMACアドレスでない場合、イーサネットフレームはルータを経由せず自ポートに到達したので、iSCSI Login リクエストを発行したポートは同一ネットワークに属する。  
判定の結果、分岐した後の処理(ステップ1120以降またはステップ1230以降の処理)は、前述の通りである。

#### 【0055】

また他の変形例について言えば、上記実施形態では、ログイン成立後も受信した各コマンドに関して、それを送信したホストをMACアドレスまたはIPアドレスを基に識別し

て、LUへのアクセス可否を判定している。これに対して変形例では、処理の簡略化または高速化などの要望に応えるために、単にログイン要求フレームの受信時に未登録のホストからのログインを拒否するだけならば、図6のステップ1420、及び又は図7のステップ1320の判定を省略し、full feature phase開始後は、受信したPDUを全てチェックせずに処理を行なうこともできる。

この場合、アクセス管理テーブル80には、単にログインを許可するホストのMACアドレスのみを登録しておけば良い。例えば図9に示すようにMACアドレスのリスト形式の登録テーブルとすれば良い。

#### 【0056】

更に他の変形例において、full feature phase(1300又は1400)で、全ての各コマンドに関して、それらを送信したホストをMACアドレスまたはIPアドレスを基に識別し、LUへのアクセス可否の判定は行わず、例えばストレージ装置200への書き込み(write)を指示するコマンドに関してのみホストのアクセス可否の判定を行ない、それ以外のコマンドはその判定を行わず処理することも可能である。

#### 【0057】

更に他の変形例において、ログアウトした後も、前回のログイン時の情報(ホストのMACアドレス、IPアドレス)をアクセス管理テーブルに記憶しておいて、次のログイン時の認証に利用することも可能である。

#### 【0058】

更に他の変形例に関して、図2を参照した上記実施形態では、ホストとストレージ装置との間のデータの通信を前提としていた。しかし、変形した例では、ストレージ装置どうしでデータ通信する場合にも適用できる。この場合、片方のストレージ装置がホストの役割を果たす。すなわちホストの役割を果たす側のストレージ装置の記憶制御装置210が持つプロセッサ270、またはホストアダプタ240が持つプロトコル処理用ハードウェア、あるいはそれらの組み合わせでホストとしてのプロトコル処理を実現する。

#### 【0059】

また他の例として、1つ又は複数のストレージ装置200にIPインタフェースを介して接続する管理サーバを設け、この管理サーバに図1示すSVP230に加え又はそれに代わって上記SVP230の機能、例えばログの記録等の処理を行わせても良い。この管理サーバにより複数のストレージ装置を一元的に監視することが可能となる。

#### 【0060】

更にまた上記実施形態では、ストレージ装置からホストのMACアドレスを獲得するためにSNMPリクエストを用いたが、別的手段を用いることもできる。例えば、iSCSIのTEXT Mode negotiation と呼ぶ、イニシエタとターゲット間で各種動作パラメータの交換をするためのプロトコルを用いて、イニシエタに対しMACアドレスを送信するように要求することができる。

その場合、SNMPマネージャやSNMPエージェントをストレージ装置やホストが持つ必要は無いが、ホストはTEXT Requestで示されたMACアドレス要求を理解し、TEXT ResponseとしてMACアドレスを応答する機能を持つ必要がある。TEXT Request及びTEXT Responseは、各々TEXT形式で記述される。

#### 【0061】

図10に、iSCSIのTEXT Mode negotiationによるMACアドレスの獲得のためのアクセス制御処理の一例を示す。

#### 【0062】

イニシエタからターゲットに対してiSCSI Login リクエストが発せられると(S1)、ターゲットからイニシエタには、iSCSI Login レスポンスが返される。この例では、MACアドレスに基づくセキュリティを利用する旨の問合せ用として、ベンダが独自に設定したXで始まるキー「X-com. . . security」をデータセグメントに用いて返信する(S2)。このようにターゲットが新しいパラメータを示したので、これに対してイニシエタは、ログインフェーズを続ける。この例では、イニシエタが、「X-com. . . security」と言うキ

ーを知っていて、「M A C アドレスに基づくセキュリティを利用する」ことに同意している。そこで、イニシエタは、ターゲットとの通信に用いるポートの M A C アドレス「0123456789AB」をターゲットへ送信する（S 3）。それを受信したターゲットは、「0123456789AB」が管理テーブルに予め設定したあった M A C アドレスであったので、ログインを許可する。反対に、もし登録されていない M A C アドレスならば、0 0 0 0 以外のステータスを応答してログインを拒否する（S 4）。

#### 【0 0 6 3】

次に、ログインの失敗した場合（B）について説明する。

iSCSI規格では、TEXT Mode negotiationにて知らないキーに対しては、イニシエタはターゲットに対して、「Not Under Stood」の値を応答する（S 3）ように規定されている。それを受信すると、ターゲットは M A C アドレスを獲得できないので、ログインを許可しない（S 4）。

このように、iSCSIのTEXT Mode negotiationを使用して M A C アドレスを獲得できる。

#### 【0 0 6 4】

以上、いくつかの実施例について説明したが、本発明は上記実施例に限定されるものでなく、その要旨を逸脱しない範囲で種々変更可能であることは言うまでもない。

#### 【図面の簡単な説明】

#### 【0 0 6 5】

【図 1】一実施形態におけるデータ処理システムのハードウェア構成を示すブロック図。

【図 2】一実施形態によるデータ処理システムにおける iSCSI のイニシエタとターゲット間の通信の概念を示す図。

【図 3】iSCSI のイニシエタとターゲット間の通信に用いられるパケットのフォーマットの例を示す図。

【図 4】ログイン要求フレームの構成例を示す図。

【図 5】図 1 に示すアクセス管理テーブル 8 0 構成例を示す図。

【図 6】一実施形態によるアクセス制御処理の詳細を示すフローチャート。

【図 7】一実施形態によるアクセス制御処理の詳細を示すフローチャート。

【図 8】一実施形態によるアクセス制御処理の詳細を示すフローチャート。

【図 9】他の実施形態によるアクセス管理テーブルの他の例を示す図。

【図 1 0】 M A C アドレスの獲得のための他の実施形態によるアクセス制御処理のシーケンスを示す図。

#### 【符号の説明】

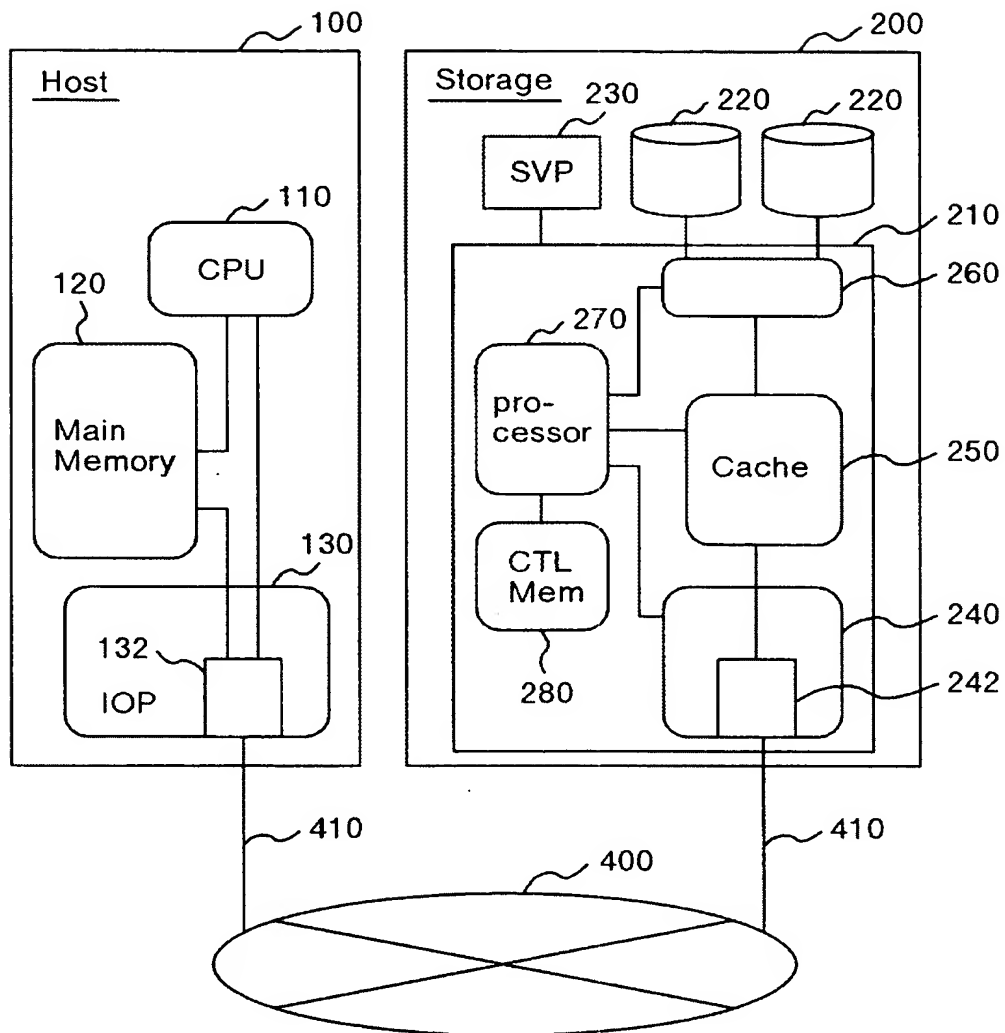
#### 【0 0 6 6】

100：ホストコンピュータ、	200：ストレージ装置
400：I P ネットワーク、	410：高速 I P インタフェース
10：ログイン要求フレーム、	20：S N M P 要求フレーム
30：S N M P 応答フレーム、	40：ログイン応答/拒絶フレーム
80：アクセス管理テーブル、	
90A：iSCSI層（イニシエタ）、	90B：iSCSI層（ターゲット）
92：T C P 層、	94：I P 層
96：M A C 層、	98：U D P 層
99A：S N M P エージェント、	99B：S N M P マネージャ

【書類名】 図面

【図 1】

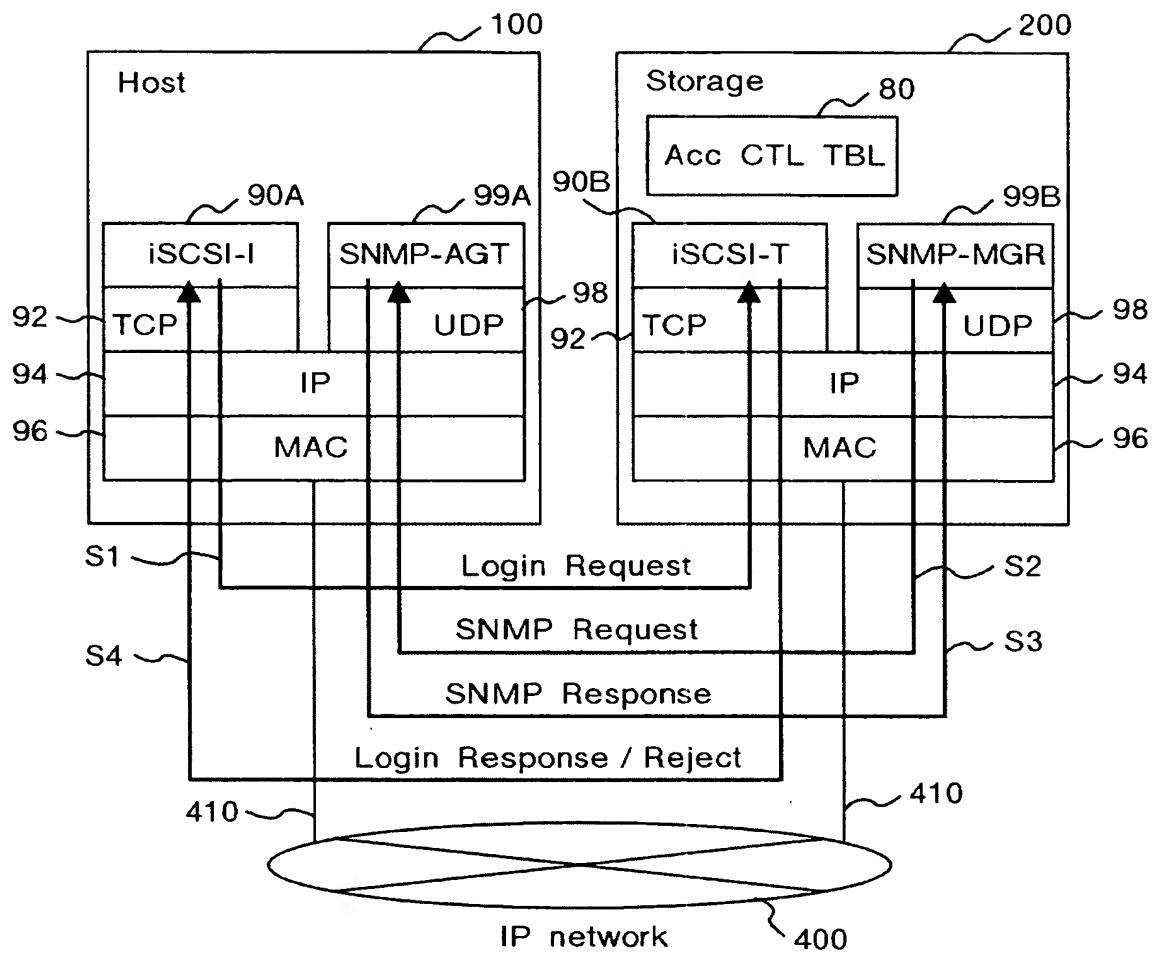
図 1





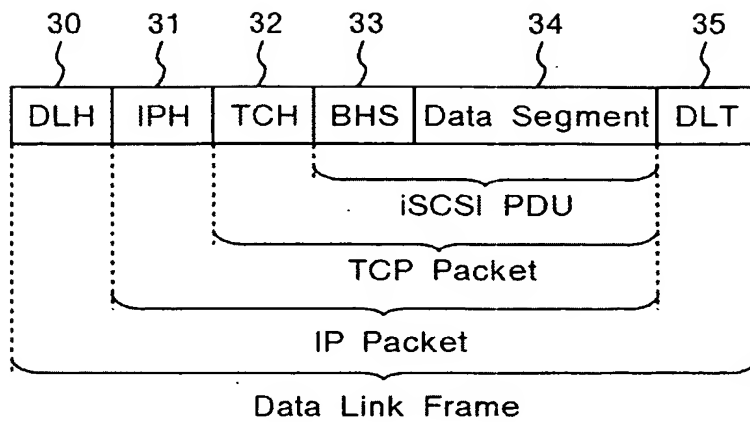
【図 2】

図 2



【図 3】

図 3

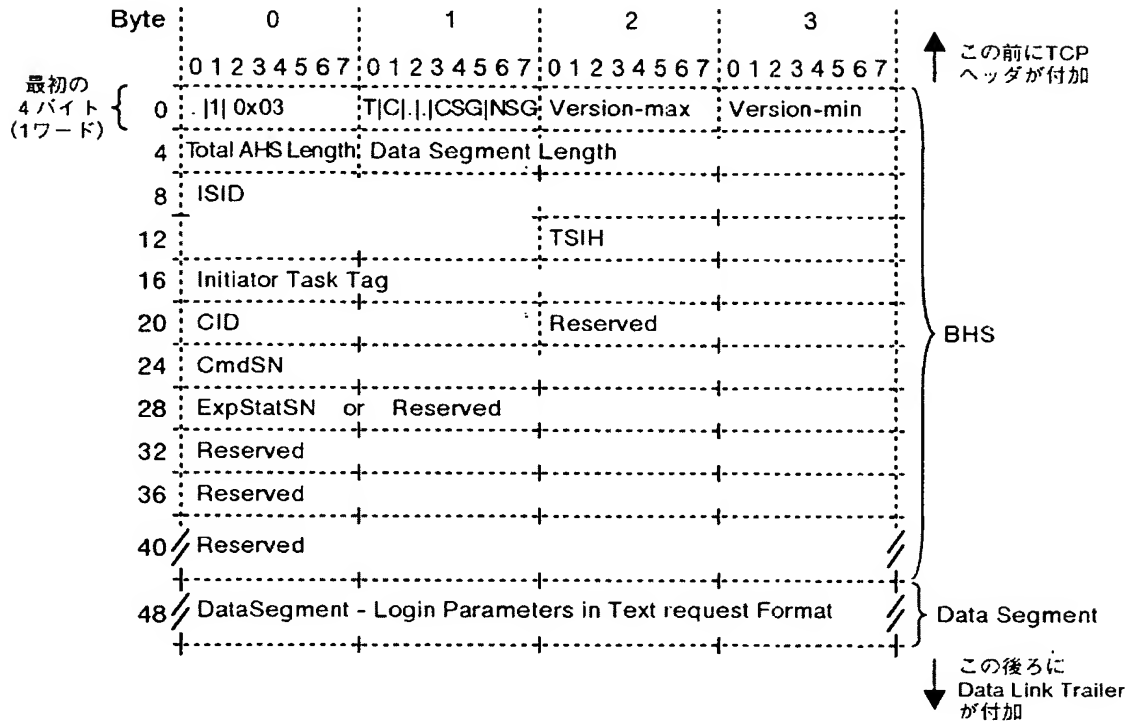


DLH : Data Link Header  
IPH : IP Header  
TCH : TCP Header  
BHS : Basic Header Segment  
DLT : Data Link Trailer

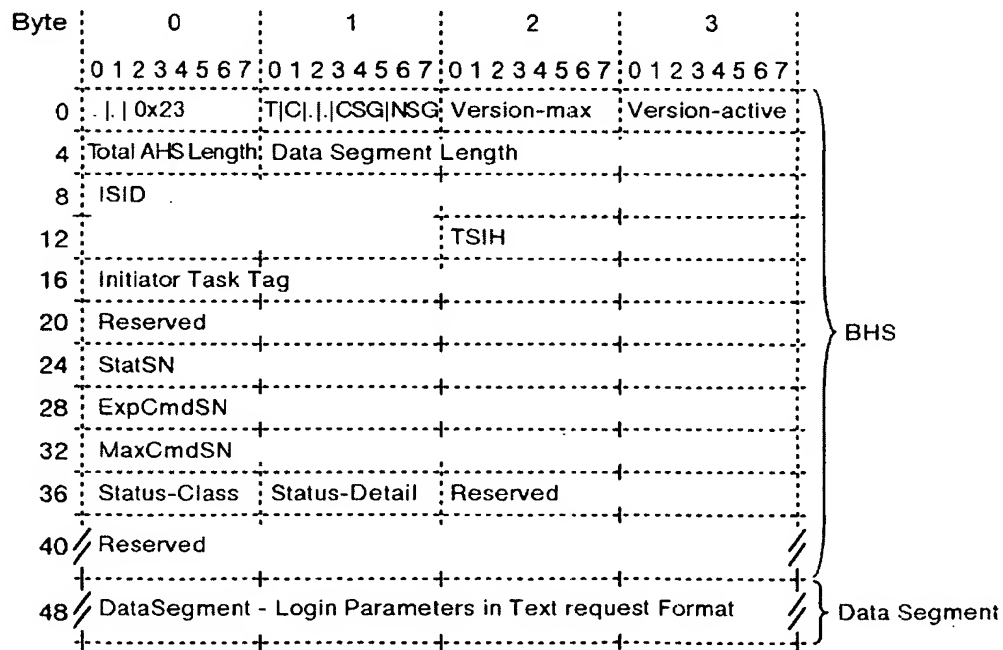
【図 4】

図 4

(A) ログイン要求 (Login Request)



(B) ログインレスポンス (Login Response)



【図 5】

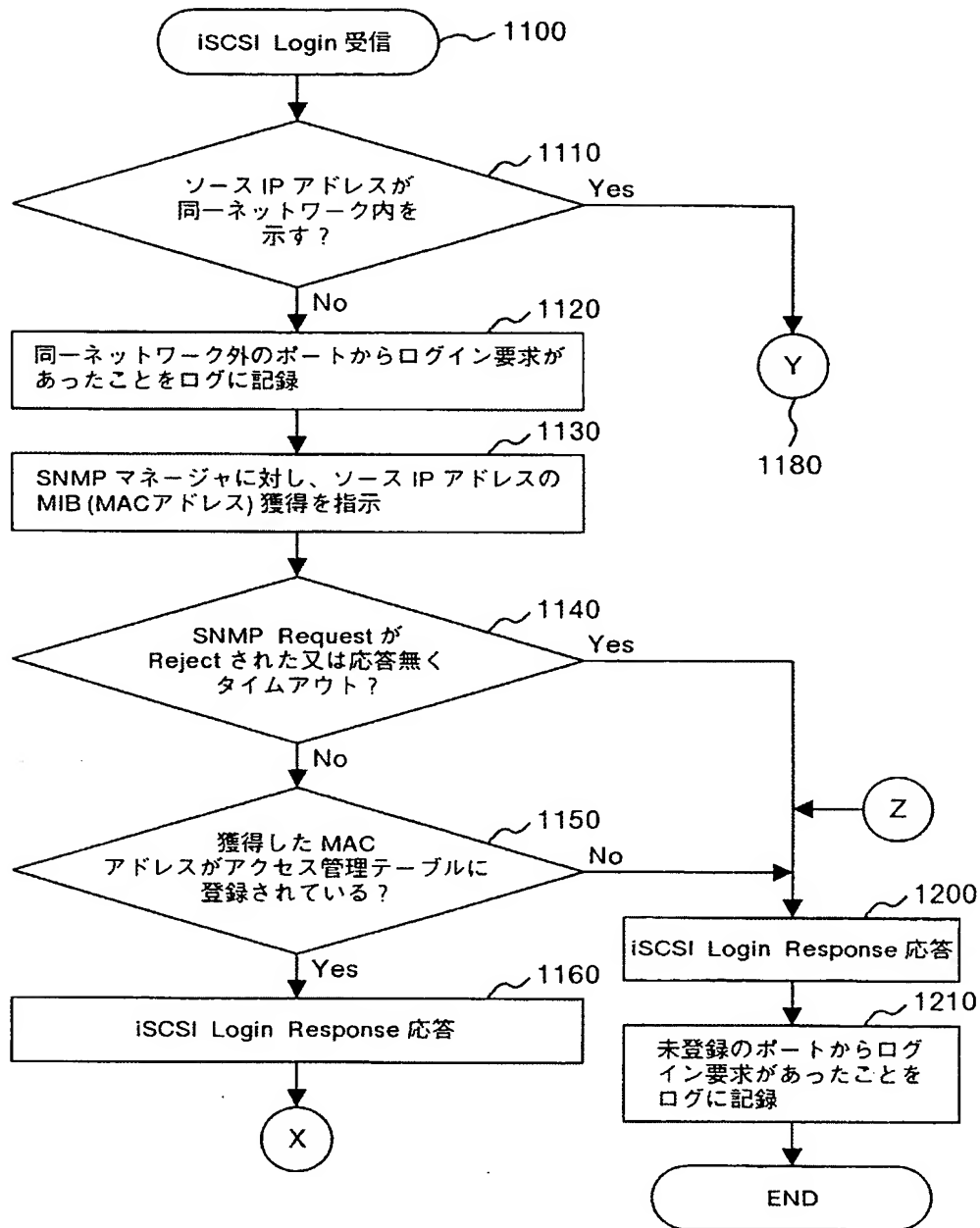
図 5

MAC Address	IP Address	LU	Session
MA0	IPA0	LUN0	establish
MA1	IPA1	LUN1, LUN2	login
MA2	nil	LUN2	Not establish

80

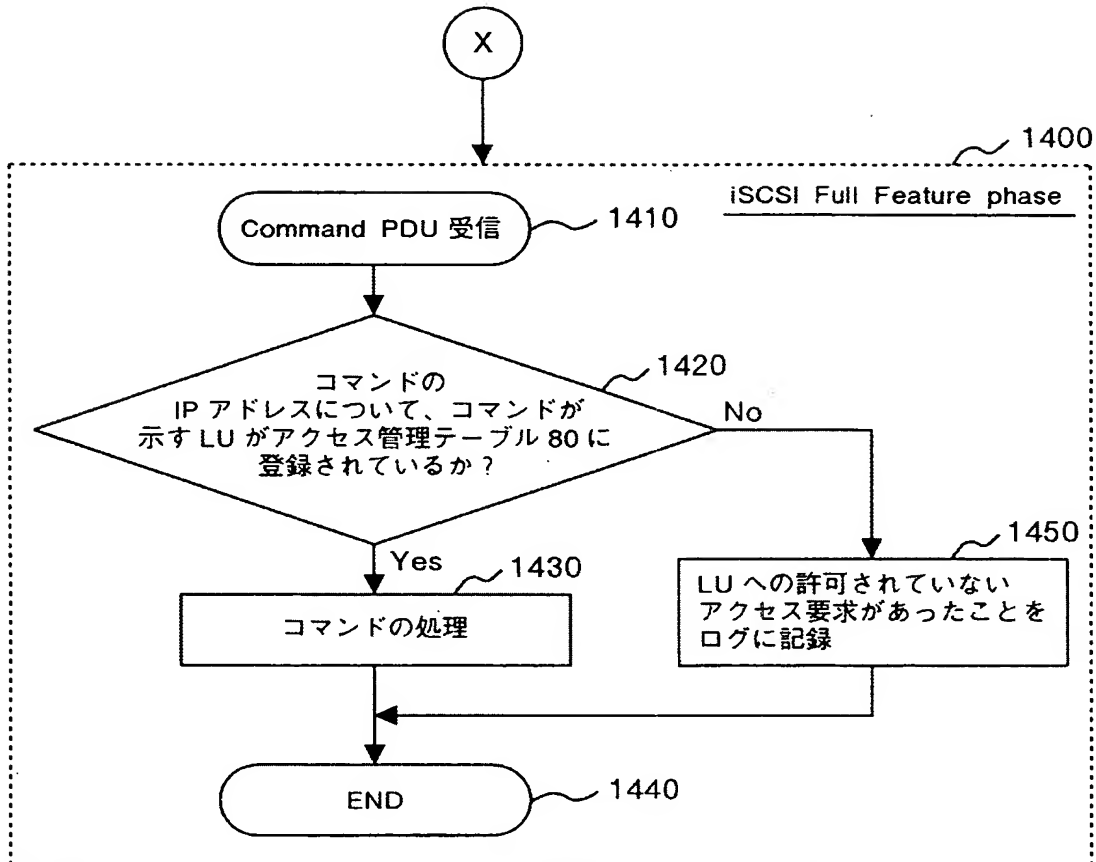
【図 6】

図 6



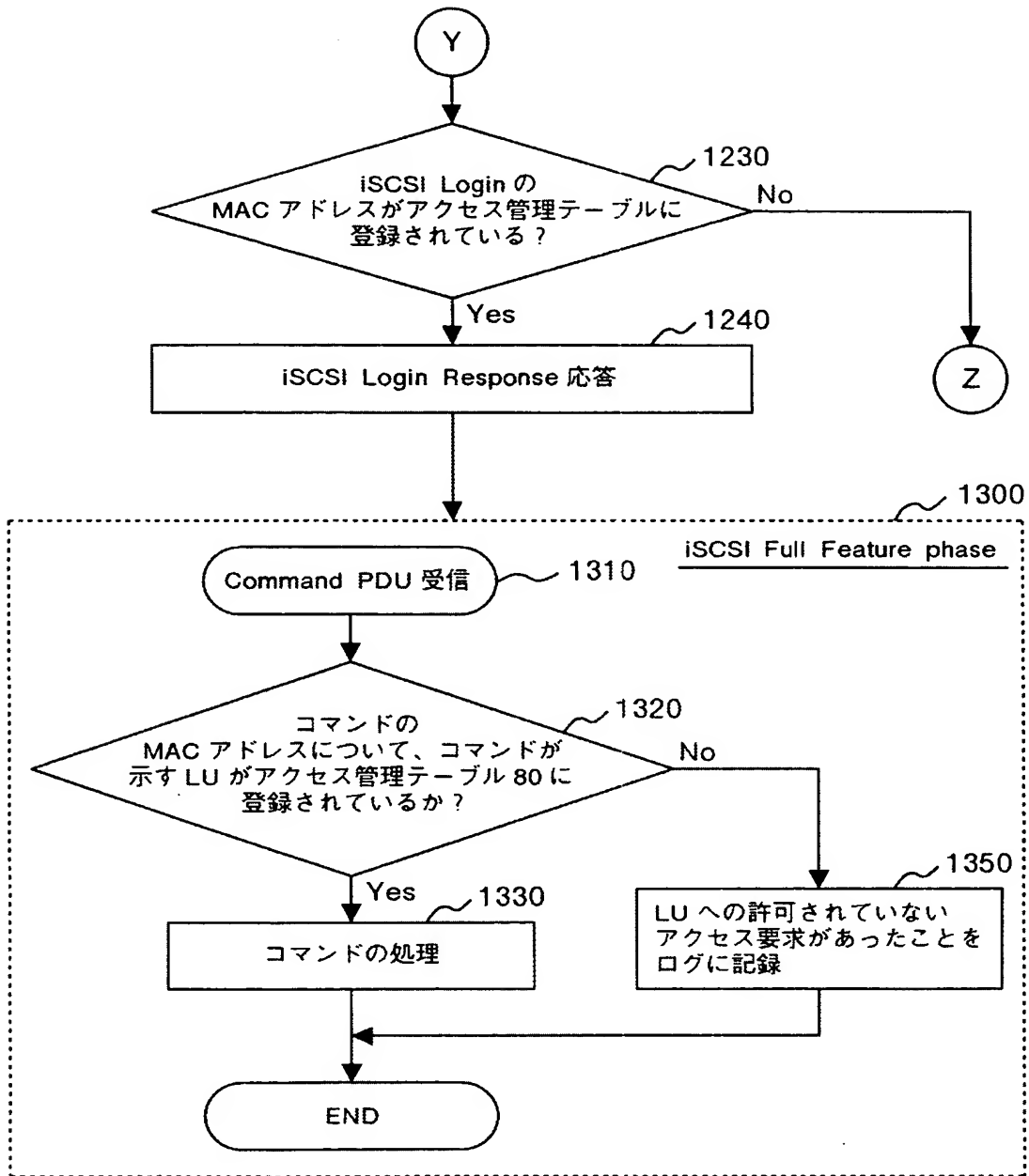
【図 7】

図 7



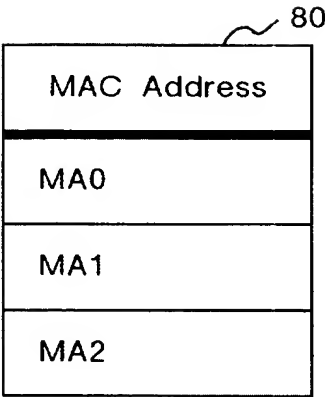
【図 8】

図 8



【図 9】

図 9

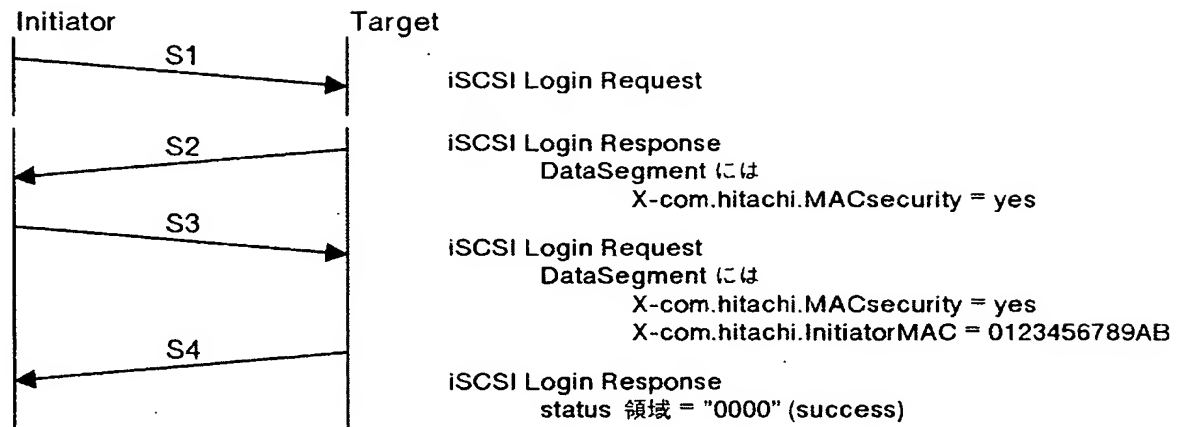




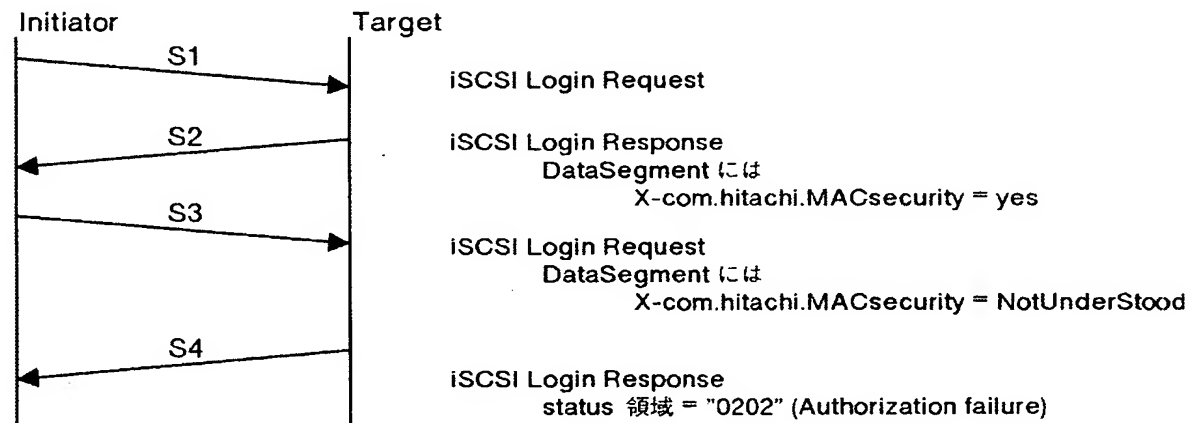
【図 10】

図 10

## (A) ログイン許可の場合



## (B) ログイン失敗の場合



【書類名】 要約書

【要約】

【課題】

iSCSI プロトコルを用いるストレージ装置へのホストからのアクセス要求に対するセキュリティの向上を図る。

【解決手段】

外部の装置からネットワークを介してストレージ装置へ送られるアクセス要求に関して、アクセス許可を管理するアクセス制御の管理方法において、外部から送信されるログイン要求のフレームをストレージ装置で受信し、受信した該フレームに外部の装置を特定する第二の情報が含まれているかを判定し（第一の判定）、第一の判定の結果、そのフレームに第二の情報が含まれていない場合、外部の装置に対してそれを特定する第一の情報の取得を要求し、取得された第一の情報に関してチェックを行い、アクセス許可をすべきかを判定し（第二の判定）し、第二の判定の結果、許可された場合に外部の装置からストレージ装置に対するアクセス要求を許可する。

【選択図】 図 2

特願 2 0 0 3 - 3 6 7 1 5 2

出 願 人 履 歴 情 報

識別番号

[ 0 0 0 0 0 5 1 0 8 ]

1. 変更年月日

1 9 9 0 年 8 月 3 1 日

[変更理由]

新規登録

住 所

東京都千代田区神田駿河台 4 丁目 6 番地

氏 名

株式会社日立製作所